## AMENDMENTS TO THE SPECIFICATION:

Please amend the paragraph beginning at page 4, line 4, as follows:

With reference to Figures 1 and 3, the approach taken by the invention is to place a secret value 10 (stored in permanent memory) into each network device that is unique to it during its manufacture (the 'manufactured key'), (stages 31 and 32 of Figure 3). This key is then used to create (stage 33) another value (the 'revealed key') that may be applied (stage 34) to the device, for example on a label 11 attached to the device. There are various suitable algorithms that can be used to compute the revealed key from the manufactured key. In some situations a digital signature checksum, such as the ones produced by the HMAC-MD5 or HMAC-SHA-1 algorithms, might be computed using the manufactured key as the secret key and some other information, such as the device serial number, one of its MAC addresses and/or a random number as input. This has the advantage of protecting much of the entropy in the manufactured key, allowing it to be used again to generate another revealed key that is unpredictable. In other situations the algorithm might be the identity function, whereby the manufactured key and revealed key are identical. Prior to installation, the revealed key is read and associated with other identification information (e.g., the device's serial number) and entered into a network or security management system that will cooperate with the device during subsequent plug and play installation. Reading the revealed key and the associated identification can be a manual process or it can be facilitated through devices such as bar code readers or text scanners.